Arithmetic Duality and Cryptography

Ming-Deh Huang
University of Southern California

Weil and Tate pairings play a significant role in cryptography.

The connection of cryptography and mathematical duality is not merely coincidental.

(1) arithmetic duality and the discrete logarithm problem

(2) arithmetic duality and pairing based cryptography.

Discrete-log based cryptography

- Probably started with ground breaking paper of Diffie and Hellman – Diffie-Hellman key exchange scheme

- Many public key cryptosystems are based on DL – El-Gamal encryption, Digital Signature Algorithm (DSA)

- Elliptic curves cryptography – new generation of DL-based cryptography, replacing $\mathbb{F}_q^*$ by $E(\mathbb{F}_q)$

Discrete Logarithm Problem (DL)

G: a finite cyclic group

α: a generator of G

$\beta \in G$

To compute a positive integer n so that $\beta = \alpha^n$ ($\beta = n\alpha$ in additive notation).

In cryptography, the order of G is a large prime ℓ.

Primary examples of G: subgroups of $\mathbb{F}_q^*$, $E(\mathbb{F}_q)$, $J(\mathbb{F}_q)$, $A(\mathbb{F}_q)$.

A candidate one-way function

$\mathbb{Z}/\ell\mathbb{Z} \to G \; a \to a\alpha$ easy to compute.

2α, 4α, ..., 2$^k\alpha$ in k doubling

Inverse is the DL problem: conjectured to be

- hard – not solvable in polynomial time
- not NP-hard either

Subexponential algorithms for DL over finite fields based on index calculus principle

1. Index calculus method gives $e^{O(\log^{\frac{1}{2}} p \log\log^{\frac{1}{2}} p)}$ time algorithm

2. Number field sieve and function field sieve methods give
   $e^{O(\log^{\frac{1}{3}} p^n \log\log^{\frac{2}{3}} p^n)}$ time algorithms
   ($n << \log p$ vs $n >> \log p$)

Length of problem $O(\log p^n)$ for $\mathbb{F}_{p^n}$.

Elliptic curve discrete-log (ECDL): DL over $E(\mathbb{F}_q)$

1. appears to be much harder than the multiplicative case

2. no effective index calculus yet

MOV reduction from ECDL to the multiplicative case using Weil pairing

Weil(Tate) pairing reduces DL over $E[\ell]$ (resp $E(\mathbb{F}_q)[\ell]$) to $\mathbb{F}_q(E[\ell])$ (resp $\mathbb{F}_q(\mu_\ell)$) is efficient in very special cases

Weil and Tate pairings were turned into positive cryptographic tools in pairing based cryptography

(Public) pairing facilitates (secret) sharing

DL is inherently related to pairing, and at a deeper level to arithmetic duality

Diffie-Hellman Key Exchange: to establish a shared secret over an insecure channel

Alice generates a random number a and sends $a\alpha$ to Bob

Bob generates a random number b and sends $b\alpha$ to Alice

Shared secret: $ab\alpha$

Alice: $a(b\alpha)$

Bob: $b(a\alpha)$

3-party key exchange using an efficient pairing $f : G \times G \to G'$

For example $f : E[\ell] \times E[\ell] \to \mu_\ell$

A, B, C generates random a, b, c resp.

Publicize: $a\alpha$, $b\alpha$ and $c\alpha$

Share: $abcf(\alpha, \alpha)$

A: $af(b\alpha, c\alpha)$

Diffie-Hellman (two-party):

Secret Sharing: Trapdoor information (a or b) makes computation easy

$\mathbb{Z}/\ell\mathbb{Z} \otimes G \rightarrow G \;\; a \otimes b\alpha \rightarrow a(b\alpha)$

Computational Diffie-Hellman Problem:

$G \otimes G \rightarrow G \;\; a\alpha \otimes b\alpha \rightarrow ab\alpha, \; \alpha \otimes \alpha \rightarrow \alpha$

3-party using a paiirng $f : G \otimes G \to G'$

Secret sharing:

$\mathbb{Z}/\ell\mathbb{Z} \otimes G \otimes G \overset{1\otimes f}{\to} \mathbb{Z}/\ell\mathbb{Z} \otimes G' \to G'$

$a \otimes b\alpha \otimes c\alpha \to af(b\alpha \otimes c\alpha)$

Bilinear Computational Diffie-Hellman Problem: given $a\alpha$, $b\alpha$ and $c\alpha$ to compute $abcf(\alpha \otimes \alpha)$

$G \otimes G \otimes G \to G'$

$a\alpha \otimes b\alpha \otimes c\alpha \to abcf(\alpha \otimes \alpha)$

Bilinear CDH problem is computing a trilinear map $G \otimes G \otimes G \rightarrow G'$ such that $\alpha \otimes \alpha \otimes \alpha \rightarrow f(\alpha \otimes \alpha)$

Need:

- $f : G \otimes G \rightarrow G'$ efficient
- $F_\alpha : G \otimes G \otimes G \rightarrow G'$ hard for all α; where $F_\alpha(\alpha \otimes \alpha \otimes \alpha) = f(\alpha \otimes \alpha)$

Implies:

- DL/G reduces to DL/G': $f_a : G \to G'$ where $f_a(x) = f(a, x)$
- CDH/G' hard: else $abf(\alpha \otimes \alpha)$, $cf(\alpha \otimes \alpha) \rightsquigarrow abcf(\alpha \otimes \alpha)$
- CDH/G hard: $a\alpha$, $b\alpha$, $c\alpha \rightsquigarrow abc\alpha \rightsquigarrow abcf(\alpha \otimes \alpha)$

Need efficient $f : G \otimes G \to G'$:

- G and G' are CDH-hard
- G is strictly weaker than G' (It is not hard to show that there cannot be an efficient isomorphism $G' \to G$ unless CDH/G' is easy.)

Natural choice of G' is the multiplicative group $\mu_\ell(\mathbb{F})$ (where $\mu_\ell \subset \mathbb{F}$).

Weil pairing and Tate pairing are natural choices (only known choices?)

DL $\rightsquigarrow$ pairing

DL $\rightsquigarrow$ local duality

DL $\rightsquigarrow$ global duality (including Index Calculus as a special case)

DL and pairing

DL over a cyclic group G of order ℓ is equivalent to computing *any* isomorphism from $G' \otimes G \to \mathbb{Z}/\ell\mathbb{Z}$.

f : $G' \otimes G \to \mathbb{Z}/\ell\mathbb{Z}$ efficient $\Rightarrow$ f_a : $G \to \mathbb{Z}/\ell\mathbb{Z}$ efficient $\Rightarrow$ DL/G easy

DL/G easy $\Rightarrow$ efficient $G \cong \mathbb{Z}/\ell\mathbb{Z} \Rightarrow G \otimes G \to G$ efficient

$G \otimes G \to G \to \mathbb{Z}/\ell\mathbb{Z}$

The CDH problem is equivalent to computing *any* isomorphism from $G \otimes G$ to G.

Mauer ('94): CDH is equivalent to DL, given an elliptic curve over $\mathbb{F}_\ell$ with $\#E(\mathbb{F}_\ell)$ smooth.

DL and local duality

$E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) \cong E(\mathbb{F}_p)/\ell E(\mathbb{F}_p)$, $\ell \neq p$ (and good reduction at p)

Tate local duality.

$$<,>: H^1(\mathbb{Q}_p, E)[\ell] \times E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) \to Br(\mathbb{Q}_p)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$$

is a perfect pairing of finite groups.

DL/$E(\mathbb{F}_p)[\ell]$ hard $\Rightarrow$ $<,>$ is hard to compute.

Efficient representation of $H^1(\mathbb{Q}_p, E)[\ell]$ and computation of $<,>$?

DL $\rightsquigarrow$ pairing

DL $\rightsquigarrow$ local duality

DL $\rightsquigarrow$ global duality (including Index Calculus as a special case)

Frey (2000):

“Hasse’s results on Brauer groups make it possible, at least in theory, to lift the problem [of discrete logarithm] to global fields … and it may well be that his celebrated sequence for global fields K and its completions K_l:

$$0 \to Br(K) \to \oplus_l Br(K_l) \overset{\sum \mathsf{inv}_l}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

can play an important role.”

Nguyen (2001): Brauer group computation and Index calculus

Huang and Raskind (04,09): Global duality and DL

ECDL and global duality

$$\begin{tikzcd}
E(K)/\ell \arrow[d] & \times & H^1(K,E)[\ell] \arrow[d] & \rightarrow & Br(K)[\ell] \arrow[d] \\
E(K_v)/\ell & \times & H^1(K_v,E)[\ell] & \rightarrow & Br(K_v)[\ell]
\end{tikzcd}$$

$$0 \to Br(K) \to \oplus_v Br(K_v) \overset{\Sigma_v \mathrm{inv}_v}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

$\chi \in H^1(K,E)[\ell]$ and $\alpha \in E(K)$,

$$0 = \sum_v < \chi, \alpha >_v \, .$$

Cassels-Tate exact sequence (more compact and refined description)

$$(**)\ E(K)^{(\ell)} \to \bigoplus_{v \in S} E(K_v)^{(\ell)} \to H^1(U, \mathcal{E})\{\ell\}^* \to Ш(E)\{\ell\} \to 0.$$

Here (ℓ) denotes completion with respect to subgroups of ℓ-power index and $\{\ell\}$ denotes the ℓ-primary part.

S: a finite set of places of K containing all bad reduction places of E and the places above ℓ.

Shafarevich-Tate group

$$Ш(E) = \mathrm{ker}[H^1(K, E) \to \bigoplus_{all\,v} H^1(K_v, E)],$$

where the sum runs over all places of K.

$Ш(E)$ is conjectured to be finite for any elliptic curve over a number field.

$\mathcal{E}$: a smooth proper model of E over an open subset U of the ring of integers of K on which ℓ is invertible and put $S = X - U$.

If $Ш(E)\{\ell\} = 0$, then from Cassel-Tate we derive:

$$E(K)/\ell \to \prod_{v \in S} E(K_v)/\ell \to (H^1(\mathcal{O}_S, \mathcal{E})[\ell])^* \to 0.$$

$$E(K)/\ell \to \prod_{v\in S} E(K_v)/\ell \to (H^1(\mathcal{O}_S,\mathcal{E})[\ell])^* \to 0.$$

Dual sequences:

$$0 \to H^1(\mathcal{O}_S,\mathcal{E})[\ell] \to \prod_{v\in S} H^1(K_v,E)[\ell] \to (E(K)/\ell)^*$$

Determining the image of $E(K)/\ell \to \prod_{v\in S} E(K_v)/\ell$ boils down to d-log problem in $\bar{E}(\mathbb{F}_p)$.

Determining the image of $H^1(\mathcal{O}_S,\mathcal{E})[\ell] \to \prod_{v\in S} H^1(K_v,E)[\ell]$ is the *signature calculus* problem.

The image of

$$H^1(\mathcal{O}_S, \mathcal{E})[\ell] \to \prod_{v \in S} H^1(K_v, E)[\ell]$$

precisely annihilates the image of

$$E(K)/\ell \to \prod_{v \in S} E(K_v)/\ell$$

under

$$\sum_{v \in S} <,>_v\colon \prod_{v \in S} H^1(K_v, E)[\ell] \times \prod_{v \in S} E(K_v)/\ell \to \mathbb{Z}/\ell\mathbb{Z}$$

Similar study on DL/$\mathbb{F}^*$ can be carried out.

From *Poitou-Tate exact sequence*:

$$0 \to H^0(G_S, \mu_\ell) \to \bigoplus_{v \in Z} H^0(K_v, \mu_\ell) \to H^2(G_S, \mathbb{Z}/\ell\mathbb{Z})^* \to$$

$$H^1(G_S, \mu_\ell) \to \bigoplus_{v \in Z} H^1(K_v, \mu_\ell) \to H^1(U, \mathbb{Z}/\ell\mathbb{Z})^* \to$$

$$H^2(G_S, \mu_\ell) \to \bigoplus_{v \in Z} H^2(K_v, \mu_\ell) \to H^0(G_S, \mathbb{Z}/\ell\mathbb{Z})^* \to 0.$$

Derive

$$H^1(G_S, \mu_\ell) \to \bigoplus_{v \in S} H^1(K_v, \mu_\ell) \to H^1(G_S, \mathbb{Z}/\ell\mathbb{Z})^* \to 0$$

Dual sequence:

$$0 \to H^1(G_S, \mathbb{Z}/\ell\mathbb{Z}) \to \bigoplus_{v \in S} H^1(K_v, \mathbb{Z}/\ell\mathbb{Z}) \to (O_S^*/O_S^{*\ell})^*$$

- DL/$\mathbb{F}^*$) vs DL/$E(\mathbb{F})$ (DL/$\mathbb{G}_m(\mathbb{F})$ vs DL/$\mathcal{E}(\mathbb{F})$)

- Feasibility of index calculus

In both cases we would like to extract tiny ”ramification signature” of a much larger object (Dirichlet character and principal homogeneous space).

We would like to be able to work with the characters and homogeneous spaces as they are involved in global and local pairings without having to explicitly construct them.

DL computation is intimately related to computation in arithmetic duality